Black Network proves its mettle during Ulchi Focus Lens 2005

LTG Thomas F. Metz, III Corps commander, GEN Leon J. Laporte, commander, Combined Forces Command Korea, GEN Kim, Third ROK Army commander, receive a battle update briefing in the III Corps TAC.

By COL Robert L. Bethea, Jr., MAJ Edward P. Mattison, Jared Shepard, and CPT Kevin Knowlen

As the Army transforms to a modular force, the dynamic nature and complexity of the signal mission environment has increased. The most significant factors involved are the influx of new technology and the diversity of missions that we are called upon to perform. III Corps G6 and the 3rd Signal Brigade addressed this growing complexity with a simple approach: "any network, any service, anywhere".

The 3rd Signal Brigade has been called upon in the last 36 months to complete a variety of missions. This included establishing and maintaining the largest combined tactical and commercial military network in United States history during Operation Iraqi Freedom II (as documented in the *Congressional Record*).

A black network is basically an unencrypted network used for the sole purpose of transmitting encrypted traffic.

More recently, III Corps was tasked with implementing and integrating a combined Defense Information Systems Agency Asynchronous Transfer Mode and commercial T1 network to support the III Corps tactical command post while deployed to Korea for Ulchi Focus Lens 2005.

The 3rd Signal Brigade also assisted in the deployment and integration of Army Signal assets and commercial assets in support of the Department of Homeland Security for hurricane relief efforts in Louisiana and Texas.

The tactical problem

Due to the rapidly changing mission, the extremely large footprint of tactical assets, and the complex commercialization process, III Corps had to integrate a multitude of transport solutions during OIF II. As a result, the requirement to have a transport independent network design became readily apparent to the officers, non-commissioned officers, and engineers of the 3rd Signal Brigade.

The transport solutions entailed deploying predominantly commercial satellite suites into hazardous tactical environments. In some instances, these commercial communications packages were not under the direct control of the military or even capable of being consistently monitored by a government agency. The need for security on these networks resulted in the

implementation of Tactical Local Area Network Encryptor, Type I, inline encryption devices across the Wide Area Network and Local Area Network environments, in both continental United States and outside the Continental U.S.

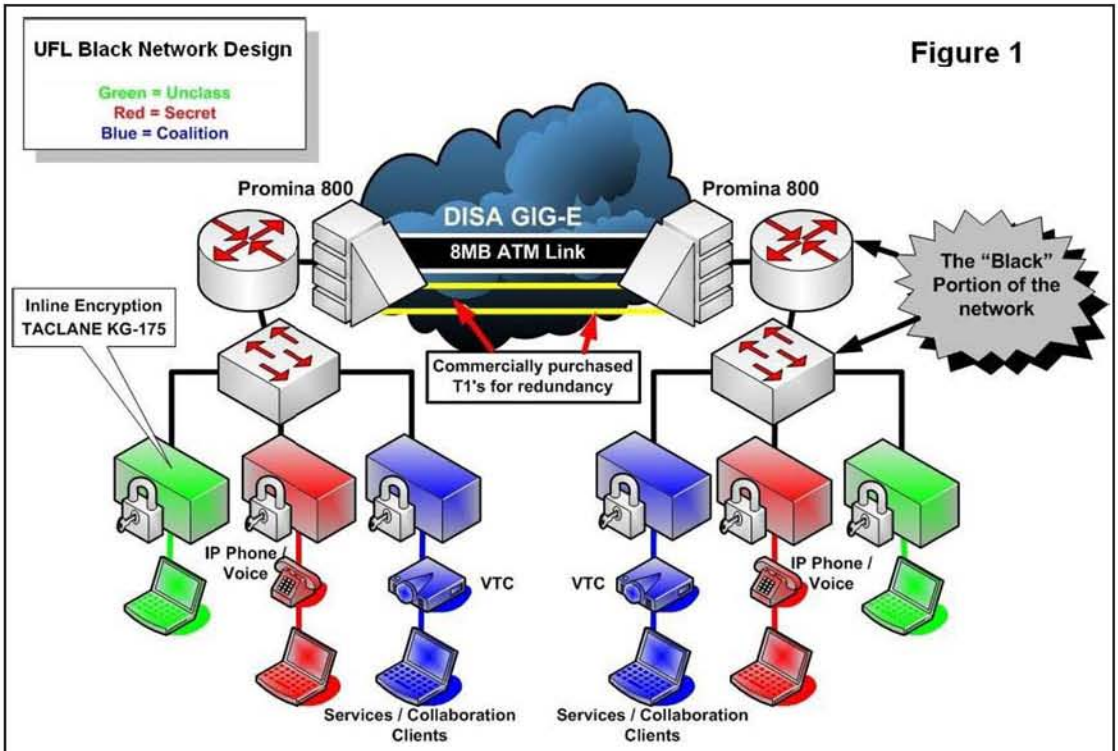

Figure 1. Black Network: this diagram shows the basic layout of how we implemented our black network. An unencrypted ATM circuit is taken from DISA and tunneled to all our tactical networks through this black pipe.

Black network design

To address this growing complexity, COL Robert L. Bethea Jr., 3rd Signal Brigade commander, directed the brigade to develop a solution independent of the transport mechanism, but still scaleable to support multiple networks (i.e.: Top Secret, Secret, Coalition, and Unclassified).

This was done through design and implementation of the black network. A black network is basically an unencrypted network used for the sole purpose of transmitting encrypted traffic. The term "black" was adopted with the intent of emphasizing that the classification of the transport network was independent of the classification of the delivered services network. The transport could be a mobile subscriber equipment node, a joint network node, a commercially purchased circuit, or even a coalition non-terrestrial package. This capability was intended to be available for major command and control nodes in Army corps, divisions, and brigade combat teams. The goal was to maintain simplicity and ease of implementation, while maximizing redundancy and efficiency for data services.

Two III Corps G6 Soldiers transport network equipment during the tactical setup in Korea for Ulchi Focus Lens 2005.

Network architecture

The Ulchi Focus Lens 2005 exercise became a perfect event to test this design due to the limited usage of Army tactical signal assets and the integration of both Defense Information Systems Agency controlled asynchronuous mode links

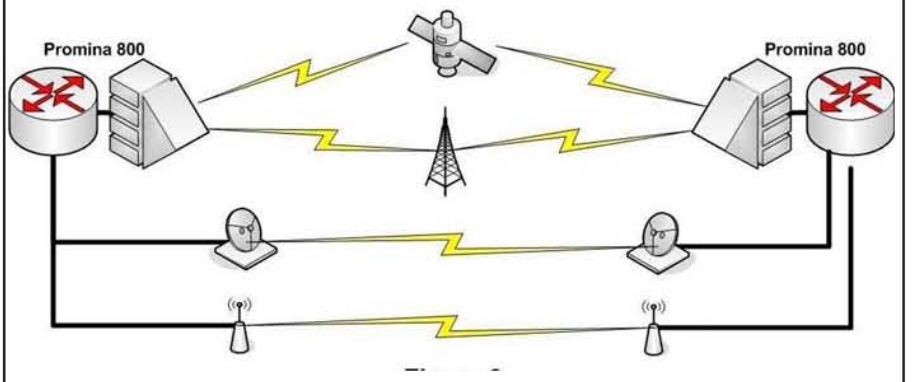

Figure 2. This diagram illustrates the black network design which is completely independent of the communication assets used for the transport method. The black network design remains the same regardless of the communication asset types used.

Tactical pit area of the III Corps TAC, where battle update briefs are received.

and commercially purchased T1 lines. 3rd Signal Brigade decided to use a Defense Information System Agency 8MB asynchronous transfer mode link and two commercial T1 lines, during this exercise, to simulate the bandwidth capacity of a Joint Node Network command post node or an ATM Moblie Subscriber Equipment node. These links were terminated at each end into Promina 800 Multiservice Access Platforms operated by the 3rd Signal Brigade. The brigade engineering team's Promina was located forward in a transit case within the III Corps tactical command post in Korea. The 57th Signal Battalion base ban node van housed the Promina in the Continental U. S. in the vicinity of the corps main command post. The raw connections for both the ATM and T1 circuits brought into the Promina are in the black network state, meaning that the classification and network provider is irrelevant to the customer's Local Area Network environment. These connections are then passed from the Promina into the black router (See Figure 1). The black router is the cornerstone of our design, acting as the central point to consolidate all IP based communications capabilities.

For this application we used a Cisco 3845 router, which allowed for both serial and Ethernet 10/100/1000 connections. This is the point where the routed relationship between any participating black routers would be established and all necessary traffic shaping could be performed. Traffic shaping at this point would be for the prioritization of one network over another, i.e., if the coalition network was the primary operational network, you could provide it the most desirable connection state.

The router is then connected to a Cisco 3560G switch via its Ethernet port, and then to each network's appropriate TACLANE device. The TACLANE device is the demarcation point for each classification's LAN network.

The main advantage of this design is the true independence of the encryption solution from the method of transport. In Figure 1, the network displayed shows the Promina being used to tie in the ATM and leased circuits, as was done during UFL 2005. However, the same design could be used with any combination of circuits and termination devices on the wide area network side of the black router; a mix of tactical assets, commercial assets, line-of-site assets, microwave, or satellites (See Figure 2) could be used. The nature and complexity of the WAN transport environment are invisible to and abstracted away from inside the LAN network.

Gateway Router Encapsulation tunnels are necessary to allow the individual network Point of Presence routers to see each other across the WAN and to exchange routes and relationships via the desired routing protocol. In a GRE tunnel environment, the PoP routers are only one hop away from each other regardless of how many hops the transport network is taking, which greatly simplifies troubleshooting. This design does not require encryption through encryption (causing additional overhead), nor does it add further complexity to the LAN environment.

(Above left) Access Layer Network Case photo: An Access layer transit case for the III Corps TAC command post is displayed. This setup for a switch and an UPS is standard for delivery network connectivity to all our subscribers.

(Above) Populated Promina 800 shows the inner workings of a Promina 800. This device was a key component of our Black network design. It served as the termination device for our ATM and T1 circuits.

(Left) VoIP Call Manager Suite photo: shows a Voice over IP transit case suite that was used in the TAC to manage our voice services provided through our IP phone network.

EoIP strategy

Another significant reason for implementing a converged black network is to eliminate the need for bandwidth provisioning. When we use traditional serial based Defense Information Systems Network WAN services, we provision bandwidth for each network or circuit individually. This bandwidth is often wasted, as it is dedicated for use by only those particular circuits or networks. For example, when bandwidth is provisioned for a serial video teleconferencing circuit and no conference is in session, the provisioned bandwidth is idle. Converged networks using internet protocol can exploit bandwidth from idle and variable sources by transmitting data from other requesting resources.

III Corps employed an "Everything over IP", or EoIP, strategy for its converged black network. EoIP technologies such as Voice over IP, IP-based VTC, and both synchronous and asynchronous collaboration tools can use the idle and variable bandwidth normally wasted by legacy circuit technology. The ability to exploit this bandwidth attracted our attention and is one of the reasons we thought it was

important to experiment with converged technology.

In our converged network implementation, we avoided bandwidth provisioning by using IP-based technologies in lieu of traditional circuit and circuit switched technologies. VoIP replaced legacy MSE voice systems. IP VTC replaced traditional serial based VTC. TACLAN E replaced circuit-based bulk encryption and provided packet encryption over the black network instead.

Results

3rd Signal Brigade chose to implement the black network design during UFL 2005 in order to simplify and maximize the performance of the communications assets provided to III Corps. This proof of concept showed that converged networking using TACLANEs (KG-175's) is a viable solution, in lieu of traditional multiplexed DISN WAN services.

The black network maintained 100 percent availability throughout the exercise. Through GRE tunneling, III Corps communicators were able to manage each of the networks supporting the corps command posts as a single virtual LAN despite physical separation on two continents. Additionally, network useage of each LAN never exceeded 85 percent across the WAN.

The black network concept has set the foundation for how future voice, video and data services will be deployed in tactical operations for III Corps. This solution is now the standard operating procedure being used in all III Corps command posts after thoroughly proving its capabilities and benefits during UFL 2005.

The way ahead

This EoIP approach worked quite well for III Corps. However, for this exercise, we did not implement quality of service measures to "protect" our high priority traffic types. As an example, in the future we want to ensure that VTC and VoIP traffic have priority over the data packets associated with email and web portals. Prior planning and the implementation of a QoS strategy could have prevented the degradation of our voice and video services we experienced when our network reached approximately 85 percent useage. Future network plans within III Corps and 33rd Signal Brigade will implement QoS by network classification and by traffic type.

The black network design functioned very well for III Corps during UFL 2005, providing a multitude of services and networks to the corps commander for the duration of the exercise. Our first attempt with converged black networking was a huge success.

Despite our lack of experience and limited QoS implementation, our network solution provided a higher standard of service than the corps staff has seen in the past.

This new standard will be expected for all future exercises, as well as the corps' next rotation to OIF.

The black network has definitely proven its mettle to III Corps!

COL Bethea, Jr. is the commander, 3rd Signal Brigade, Fort Hood, Texas. He earned a Bachelor's of Science degree in electronics and technology from Norfolk State University. He previously served as the Multi-National Corps Iraq ACofS C6. He also previously commanded the Joint Communications Support Element, MacDill Air Force Base, Tampa, Fla.

MAJ Mattison is the deputy corps automation officer, III Corps, Fort Hood, Texas. He earned a Bachelor's of Science degree in computer science from Binghamton University. He previously served as the Data Services Manager for Multi-National Corps Iraq.

Mr. Shepard is an employee of Blackhawk Management Corporation. He serves as the Technology Planner for III Corps ACofS G6, Fort Hood, Texas. He earned a Bachelor's of Science degree in Computer Science from Trinity College.

CPT Knowlen is the brigade telecommunications officer, 3rd Signal Brigade, Fort Hood, Texas. He earned a Bachelor's of Science Degree in Administration from Baylor University.

Acronym QuickScan

ATM – Asynchronous Transfer Mode
BCT – Brigade Combat Team
BNN – Battalion Base Ban Node
C2 – Command and Control
CONUS – Continental United States
DISA – Defense Information Systems Agency
DISN – Defense Information Systems Network
EoIP – Everything over Internet Protocol
GRE – Gateway Router Encapsulation
IP – Internet Protocol
JNN – Joint Network Node
LAN – Local Are Network
LOS – Line of Sight
MCP – Main Command Post
MSE – Mobile Subscriber Equipment
OCONUS – Outside the Continental United States
PoP – Point of Presence
QoS – quality of service
TAC – Tactical Command Post
TACLANE – Tactical Local Area Network Encryptors
UFL – Ulchi Focus Lens 2005
US – United States
VoIP – Voice over Internet Protocol
VTC – video teleconferencing
WAN – Wide Area Network